Turning Access Into Recurring Revenue

Offering security as a service (SaaS) can allow installing contractors to break out of the binds of a project-based existence. Access control is an area that especially lends itself to service-based RMR. Learn about the exciting varieties now available. **By Al Colombo**

ACCESS CONTROL ranks among the top three revenue achievers in the security market today. And now that a significant portion of the industry is finally embracing managed and hosted access control, new sources of recurring revenue have emerged for security integrators and alarm dealers. This access business model, however, is not new to the security industry.

Kastle Systems of Arlington, Va., has offered managed access control since the 1970s. In 2009, Gene Samburg, the founder of Kastle, said, "I believe that the manage-access philosophy works. Kastle manages 1,700 office buildings, 280 million square feet of real estate, with 1.7 million cardholders — so we must be doing something right."

Today, the company claims it protects more than 2,000 properties with in excess of 37,000 tenant spaces, totaling 400 million square feet of office space. The fact is managed access has always been Kastle's claim to fame and now here we are, three-and-a-half decades since the firm began offering this unique service, on the cusp of industry-wide acceptance. What a tribute to Samburg's forward vision.

"We offer managed access, hosted, as well as centralized client server-based access control. It is our belief that the market has accepted it as the next big thing in access control," says Michael Perlow, sales director with Idesco Corp., a New York-based security integrator.

There are also equipment manufacturers that have been experiencing an increase in managed and hosted access equipment purchases every year. "At Brivo, we have seen a 30% increase in the purchase of cloud-based managed/hosted systems each year for the past 16 years," says Lee Odess, vice president of marketing with Brivo Labs of Bethesda, Md. "I would say use of hosted systems is sure to increase as more and more security companies see the profit potential."

Let's take a look at the different flavors of access control offerings along with the advantages they present integrators, with particular attention directed at cloud-based services.

Emerging Access Business Models

There are several access business models that security integrators commonly follow. They are: traditional; hosted; managed; and lease purchase.

In a traditional, on-premises access control system the network head-end, which includes a PC or server, the software and data storage devices are contained onsite where they connect to a series of controllers that communicate with card readers, relay banks, and other building subsystems. The access control system may or may not be part of the facility LAN (local area network). Of course, there are advantages and disadvantages to this approach, which we'll cover a little later.

Hosted access systems are different in that all head-end components, like the main server, software and data storage device(s), are contained off-premises — typically within a cloud. Using this model, the client pays for the use of these components while retaining ownership of access controllers and other peripherals onsite. The security integrator usually offers this service to the client through a third-party arrangement, thus it's the integrator/host provider's responsibility to pay all costs associated with maintenance and replacement.

A managed access system, on the other hand, involves the day-to-day operation of an access system by professionals for a recurring fee, whether it's by the month, quarter, semi-annual or annual in nature. In years past, some security integrators provided several levels of managed services using the traditional access model. This includes database management card/token issuance, badging and card/token revocation. Today, many of these same companies provide these same services using the cloud model.

The lease purchase model is simply an arrangement between the security integrator and end user that allows the latter to pay for and eventually own the head-end equipment. Of course, this approach includes both traditional and cloud models, and it may or may not include the access control peripherals onsite. There are no limits to the number of combination of business models that the integrator can come up with, and it all involves budget, sales concept to the client and recurring revenue.

Advantages on All Sides

There are advantages to each access model for both the client and the security integrator. For example, using the traditional model, where the client typically owns it all, from the network head-end to the access control peripherals, the advantage to the client is

7 Flavors of 3rd-Party Services

Following is a list of various service models in common use today:

1. Access Control as a Service (ACaaS) Clients rent service instead of purchasing it

2. Software as a Service (SaaS) Current version of a particular software is accessed in the cloud

3. Security as a Service (SaaS) Client's security needs are provided as part of a larger service

4. Integration Platform as a Service (IPaaS) Hosting company integrates applications via the cloud

5. Infrastructure as a Service (IaaS) Provider outsources infrastructure as a service

6. Platform as a Service (PaaS) Host provides software, PC, servers and infrastructure

7. Database as a Service (DaaS) Third party stores access control database in the cloud

Michael Perlow, sales director with Idesco Corp. of New York, contributed to this sidebar.

Cloud storage used to be a joke within the CCTV community, but increasingly it really is a viable option for security.

that they pay for the equipment upfront without monthly, quarterly, or yearly fees — other than a possible maintenance contract.

Although this saves money in the long term for the client, it saddles them with the responsibility of paying all maintenance fees as well as device replacement as the system approaches end of life. The advantage for the security integrator, on the other hand, is a source of recurring revenue that adds to available cash on hand as well as the year-end bottom line.

"We have [an access control] solution for everyone with a lower cost of ownership, higher reliability and more current software than their existing security platform can offer," says Perlow. "In order to make this happen, however, we've had to re-educate our [traditional] clients on what managed and hosted access control can do for them and what resource it will free up for them internally."

The advantage of hosting the access control system in the cloud is that it provides a more flexible, on-demand environment than a traditional, on-premises system. Cloud-based access enables the client or the security integrator to change head-end characteristics, storage capacity and add additional services on the fly. The system can be reconfigured in real-time without human intervention through a control panel that resides with the head-end in the cloud. Herein lies one of the most powerful advantages afforded using the hosted model in the cloud.

There are numerous combinations involving hosted and managed access configurations. An access control system can be hosted in the cloud while the client manages their own day-to-day affairs. The security integrator can provide minimal operations support by adding card/token credentials, removing additional ones, adding or deleting users, and more. A third-party service could also provide hosting, management, and other services as needed — all of them through the security integrator.

Note that software also can be offered as a service to the client, referred to as SaaS (software as a service). When the software development setting is provided to a client, it's called PaaS (platform as a service); and when the hardware is offered as a service it's usually referred to as IaaS (infrastructure as a service). For a complete list of current "as a service" offerings, see the sidebar.

Security in the Cloud

With all the security concerns involving network hacking in the news, many security integrators are left scratching their heads, wondering whether the cloud is secure enough for their client's needs. When you read about the huge losses experienced by really big retail stores, such as Target, Home Depot, Neiman Marcus, as well as motion picture giant Sony, to name only a few, it's understandable why integrators are concerned.

According to NIST (National Institute of Standards and Technology), the use of cloud computing is a lot like that of wireless communication when it first came into fashion for sending voice and data from one point to another. Over time, government agencies and private corporations learned how to better protect their data and communication path. The same process is repeating itself with cloud technology, and there are ways to assure that the client receives the best secure cloud service available.

According to cloud access security broker Bitglass, "It's the job of SaaS application providers to ensure that their products are as secure as possible. After all, they're asking enterprises to trust them with their data, which is highly valuable. Many SaaS vendors hire the best and the brightest in IT security, and buy the best security products in order to ensure the security of their customers' data."

The question is how can security integrators and alarm dealers know which cloud products to use? Brivo's Odess offers some sound advice.

"A good way to assure that you get the most secure cloud service possible is to ask the right questions," he says. "Ask the provider if they use sophisticated encryption. What is the

provider's SOA [standard operating arrangement] if the system should go down? What's the service agreement like? You can tell those who are faking it. We hire white-hat hackers to find holes we may have in our system — it's a core part of who we are and how we do business."

Ask the provider to put it in writing how they prevent hacking from taking place. If they won't put it in writing, Odess says to run in the opposite direction. Also, ask the provider what the device communication protocol is in the wild that communicates with the host. How is this information communicated? Is it always open or does it periodically call home? Is it encrypted and how do they manage this encryption (certificate/SSL)?

"How do you manage the info that is being shared? Is it in the cloud, and if it's there, where is it hosted at [physical location]. Another thing is just because the colocation facility [that backs up the data] has a rating does not mean their stack has a rating," says Odess. "If they use IaaS [integration as a service], which one are they using and how is it protected?"

There are two types of clouds in use —private and public. Government and high-risk commercial should opt for a private cloud environment simply because the entire cloud is dedicated to the needs of just that one entity. However, the cost of a private cloud offering sometimes is considerably higher than that of a public cloud. High-risk applications may warrant the use of a private cloud offering so there is no chance of data compromise.

For more information on how to determine the quality and security of a cloud provider, go to microsoft.com/industry/government/guides/cloud_computing/3-security.aspx.

Tooling Up for the Cloud

What does a traditional security integrator or alarm dealer have to do to enter the managed/hosted access control arena? The answer is, according to Odess, "Not a whole lot. It does help to understand basic IT. Integrators need to understand network terminology as well as the IT implementations. They also need to know cloud computing and how hosted architecture works."

According to Idesco's Perlow, dealers need to know networking as well as the various ROI (return on investment) drivers associated with cloud services. In addition, they need to know and understand the structure of the particular cloud that the provider has set up for its use.

"As an integrator we need to know network configurations, why these configurations are better for the client in the long run, and how safe the solution is that we propose to provide our client with. Our reputation and ability to provide solutions are hinged on all three," he says.

Cost of implementation of a cloud-based, managed/hosted access system may actually be less than you think. Probably the biggest need is education, although most security integrators already have a basic knowledge of network technology. The particulars associated with traditional and cloud-based IT are not all that different.

Sales personnel must also refashion their thinking to include cloud-based applications. For example, how exactly do you identify a client whose access needs lend themselves to the use of managed or hosted access control services? The fact is almost any size or type of company or government entity qualifies as a cloud client.

"Anything from small businesses to property management companies to hospitality and retail [is a prospect]," says Odess. "It really goes across all verticals. What we see is an enormous trend in the SaaS model in multitenant applications to manage them via the Internet using an ordinary Web browser."

It all boils down to ease of management, user operability, detailed reports, as well as implementation of the various cloud-based access control models, but in the same types of applications, whether it involves managed or hosted services. Odess says 90% of all security applications fit the cloud model, whether it involves hosted, managed, leased, with or without SaaS, or any combination thereof.

"The question is, is the integrator building a lifestyle business or just a business?" says Odess. "It's a matter of preference and how you want to create value for your organization. That's different than how the client sees it but it's an important question for the integrator to consider." SSI

AL COLOMBO (allan.colombo@yahoo.com) is a long-time trade journalist and copywriter in the electronic security market. His experience includes 15 years as a field technician and 28 years in technical writing.

Why Self-Managed Security Can Be Dangerous

One of the most difficult access control systems to administrate for end users is one that contains biometric identifiers as well as video for verification. On the access side, this includes systems that utilize hand geometry, thumbprints, voiceprints, retina/iris scans and any other flavor on the market. According to some experts on biometric access, the problem is the day-to-day administration that a biometric access system requires, which includes enrollment, authentication and validation. On the video side, this includes real-time, operator-monitored, onsite systems.

Using an office building as an example, the building operator is an office building operator, not a security expert. Operating the day-to-day business of an office building is what this person does best and it's how they make their living — not enrolling, programming and administering access control and video surveillance systems.

The problem in this respect involves the human element. Flaws in logic and decision making can adversely influence outcomes where people are involved, especially untrained users who do not work with access control on a daily basis. Mistakes also can occur in user-administered system programming that can negate the fundamental advantages of access and video, especially where it involves biometric credentials.

For example, mistakes in judgment can occur when an end user looks up something to assure identity. Issuing and administering biometric credentials in this regard can pose a tremendous challenge to some users. And when you add human judgment in the security decision-making chain, you weaken that chain. User-managed video systems, for example, are good for archival where you can go back and put it all together, but to try to monitor what's going on in real-time in order to make informed decisions, that's not what the end user should be doing.

This is precisely why managed access control makes sense.